

**UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND**

**IN THE MATTER OF THE
SEARCHES OF**

**THE PREMISES
COMMONLY KNOWN AS:
1318 SALONICA PLACE
BEL AIR, MD 21014**

**A 2016 DODGE MINIVAN WITH
MARYLAND TAG 7CX2823**

**A CHEVROLET PICKUP TRUCK WITH
MARYLAND TAG 14X066**

✓

* FILED * ENTERED UNDER SEAL
* LOGGED * RECEIVED

20 - 0810 BPG

MAR 24 2020

CASE NO. _____

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND DEPUTY

20 - 0811 BPG

BY *OKS* *

CASE NO. _____

20 - 0812 BPG

* * *

CASE NO. _____

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kelly M. DiAntonio, being duly sworn, depose and state that:

1. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”) since April 2012. As part of the daily duties as an HSI Special Agent, your Affiant investigates criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, U.S.C. §§ 2251 and 2252A. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received formal training through HSI, and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material, and internet crime. I have participated in the execution of numerous search warrants, of which the majority has involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for

computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the HSI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PURPOSE OF THIS AFFIDAVIT

3. This affidavit is made in support of an application for search warrants to search:
- a. The entire premises located at **1318 Salonica Place, Bel Air, Maryland 21014 (SUBJECT PREMISES)**, more specifically described in Attachment A1, which is incorporated herein by reference;
 - b. A **2016 Dodge Minivan with Maryland tag 7CX2823**, more specifically described in Attachment A2, which is incorporated herein by reference; and
 - c. A **White Chevrolet Pickup Truck with Maryland tag 14X066**, more specifically described in Attachment A3, which is incorporated herein by reference;
- collectively referred to in this affidavit as the “**TARGET LOCATIONS.**”
4. The purpose of this application is to seize evidence of violations of 18 U.S.C. § 2252A(a)(2), which prohibits the distribution and receipt of child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which prohibits the possession of child pornography.

5. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 2252A(a)(2)(distribution and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B)(possession of child pornography), are located within the **TARGET LOCATIONS.**

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS
AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND
THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION
OF CHILD PORNOGRAPHY**

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films,

video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept in a location controlled by the collector, usually at the collector's residence, or in online storage, email accounts, or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials about the sexual interest, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts, or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Certain communication "app" environments also include chat rooms that cater, wholly or in part, to those with interest in child pornography or the sexual exploitation of children. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way child pornography is produced, distributed, and utilized. It has also revolutionized the way child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom

facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images are now transferred directly onto computers. Modems allow any computer to connect to another computer through a telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornography can be transferred via electronic mail, file transfer protocols (FTP), or other communication pathways to anyone with access to a computer (including mobile telephones) with access to a data network. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

f. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo! and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer (including many telephones) with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

g. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

h. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the production, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

i. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

j. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

k. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

l. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

m. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above described information will be recovered during forensic analysis.

KIK

8. Kik Messenger, also called Kik, is an instant messenger application for mobile devices. Kik Messenger lets users send text, pictures, videos, sketches, and other files within the

Kik app to an individual user or a group of users. Kik allows users to create a free account using an email and a password. Kik uses usernames to identify their users. A Kik username is the only unique identifier in the Kik system, and the only way Kik can identify a unique Kik account. Kik usernames are unique to each account and cannot be duplicated. Additionally, when a Kik account is suspended, deactivated, or deleted, the Kik username cannot be recycled. Kik uses an existing Wi-Fi connection or data plan to send and receive messages. Kik Interactive was previously located in Ontario, Canada but has recently been purchased by MediaLab; a U.S. based company. Kik did not retain chat communication and Kik only retained IP addresses and content for the past 30 days.

9. Based on my knowledge and experience, the Kik application can be downloaded onto a smartphone and can be accessed virtually anywhere. Additionally, I am aware that smartphones are relatively small in size and can be secreted in many places to include on a person, in a residence, or in a vehicle.

PROBABLE CAUSE

Overview of the Investigation:

10. This investigation has revealed that an individual or individuals residing at **1318 Salonica Place, Bel Air, Maryland 21014** (the **SUBJECT PREMISES**), is/are using the Kik username “Rvpwk” to receive and distribute child pornography.

11. In October 2019, HSI Baltimore received information from HSI Ottawa, regarding Kik user “Rvpwk,” who was receiving and distributing visual depictions of minors engaged in sexually explicit conduct in a Kik group. HSI Ottawa received information from the RCMP National Child Exploitation Coordination Centre (NCECC) containing a chat log between users, discussing having sexual intercourse with a minor. One such user, “rvpwk,” implied that they were a teacher who was going to have sexual intercourse with a 15-year-old

student in exchange for a grade change.

12. The following conversation occurred in the private Kik group “Good Shit” on or about September 16, 2019.

Date/Time:	Chat:	Sender:
9/16/19 03:03:46 UTC	“You guys, I’m excited”	“rvpwk”
9/16/19 03:04:10 UTC	“I might get to fuck a student for a grade bump”	“rvpwk”
9/16/19 03:04:31 UTC	“How old”	***Redacted_10***
9/16/19 03:04:35 UTC	“What ages you teach?”	***Redacted_6***
9/16/19 03:04:50 UTC	“I’m a high school teacher, she’s 15”	“rvpwk”
9/16/19 03:05:02 UTC	“A bit old imo, but kids are kids”	“rvpwk”
9/16/19 03:05:26 UTC	“Did she suggest it or you?”	***Redacted_1”
9/16/19 03:05:33 UTC	“She did”	“rvpwk”
9/16/19 03:05:46 UTC	“Likes to hang out in my room at lunch”	“rvpwk”
9/16/19 03:06:27 UTC	“She has a D and it's the 3rd week, so she needs it”	“rvpwk”

13. On or about September 16, 2019, just prior to the conversation, Kik user “Rvpwk” posted a video file utilizing IP address 174.205.13.9. I have reviewed the video file “Rvpwk” distributed to the Kik group and it is named and described as follows:

1ad5d5c6-71a4-4929-9378-cadb5efba0db – a video approximately one minute and twenty-two seconds in length, depicting a minor female lying face down on a white sheet with her butt in the air. She is wearing only a pink shirt with a pattern, that is pulled up, exposing her back. The minor female is being penetrated by the erect penis of an adult male.

This video is determined to be child pornography as defined in Title 18, United States Code, Section 2256(8).

14. On or about September 16, 2019, immediately following the above-referenced

conversation, Kik user “666filia” posted a video to the same Kik group to which “rvpwk” remained a member. I have reviewed the file posted and it can be described as follows:

d23458a7-9e2f-4662-90bf-74e958bf6338– a video approximately twenty-three seconds in length of a minor female masturbating and then performing oral sex on a prepubescent male.

This video is determined to be child pornography as defined in Title 18, United States Code, Section 2256(8).

15. The Kik records reflect that “Rvpwk” shared the child pornography file referenced in paragraph 13 above on September 16, 2019 at 03:22:02 UTC, from IP address 174.205.13.9. This IP address resolved back to Verizon Wireless. Subscriber information for mobile IP addresses cannot be directly connected to an individual account and mobile providers retain little or no data relating to IP addresses. Additionally, even if a mobile provider retains IP data, the IP address cannot be connected to a single account, the way a residential land-based IP address can be (such as Comcast or Verizon FIOS accounts). In other words, multiple mobile users can be accessing the internet from the same IP address.

16. Information was received from Kik pertaining to the account “Rvpwk,” including subscriber information, account data, service data, and recent IP addresses. The following information was provided for the Kik user “Rvpwk”:

First Name:	Rvpwk
Last Name:	Qwerty
Email:	rmomgay69@gmail.com (deactivated_unconfirmed)
Username:	rvpwk
Registration:	2019/07/13 04:52:18
Country-code:	US
Device-type:	android

17. Kik also provided IP logins for Kik user “Rvpwk” from September 8, 2019 through and including September 16, 2019. There were over 120 logins to this account during the 8 days referenced above. Between, September 8, 2019 and September 16, 2019, IP address

71.166.36.183 was used to access the Kik account of “Rvpwk” in over 90 instances. On September 16, 2019, around the time of the receipt and distribution of the videos and conversation that took place, Kik reported the following account activity:

Date:	Time:	IP Address:	Chat Network:
2019-09-15	21:58:57 UTC	71.166.36.183	WIFI
2019-09-16	02:52:49 UTC	174.205.13.9	MOBILE-LTE
2019-09-16	03:25:50 UTC	71.166.36.183	WIFI

18. An administrative summons was sent to Verizon Internet Services for subscriber information for IP address 71.166.36.183 on September 16, 2019 at 23:03:06 UTC. This was the most recent, non-mobile IP address utilized to access the Kik account “Rvpwk” using wifi.

Verizon responded to the summons with the following subscriber information:

Subscriber Name: Patricia Daniels
Service Address: 1318 Salonica Place, Bel Air, MD 210140000
Daytime Telephone: 4439870296
Account Status: Active

IP Session Details:

IP Address: 71.166.36.183
Start Time: 2018-10-31 07:32:47z
Stop Time: Still assigned on the date of the request

19. In February 2020, HSI Baltimore received a packet of leads pertaining to Kik users who were flagged as having distributed child pornography in September 2019. One of these leads contained information on Kik user “rvpwk.” The new lead contained the following information from Kik:

First Name: Rvpwk
Last Name: Qwerty
Email: rmomgay69@gmail.com (deactivated_unconfirmed)
Username: rvpwk

Registration: 2019/07/13 04:52:18
Country-code: US
Device-type: android

20. On or about September 14, 2019 at 12:49:46 UTC, in a private Kik group with the group name “Nunrulz,” user “rvpwk” shared a video with content ID: 9dd017e8-9b0e-4c31-a19f-917b76bc29d0. The IP address utilized to upload the video was 71.166.36.183, **the IP address assigned to the Target Premises**. I have reviewed the file posted and it can be described as follows:

9dd017e8-9b0e-4c31-a19f-917b76bc29d0—a video, approximately eight seconds in length, of a prepubescent female wearing pink and white bottoms who is being vaginally penetrated by the erect penis of an adult male. The minor female is straddling the adult male’s lap and he is holding on to her stomach and bottoms as he thrusts his penis into her vagina.

21. In February 2020, HSI Baltimore sent a summons to Verizon Wireless, pertaining to the IP address 71.166.36.183 on September 14, 2019 at 12:49:46 UTC, the time of the video upload. Verizon responded with the following information:

Subscriber Name: Patricia Daniels
Service Address: 1318 Salonica Place, Bel Air, MD 210140000
Daytime Telephone: 4439870296
Account Status: Active

IP Session Details:

IP Address: 71.166.36.183
Start Time: 2018-10-31 07:32:47z
Stop Time: Still assigned on the date of the request

22. A public database search of the address 1318 Salonica Place, Bel Air, Maryland 21014 revealed the **SUBJECT PREMISES** is owned by William Thomas DANIELS II. Queries conducted through Maryland Wage and Earnings revealed that William DANIELS II is currently employed by Enterprise Electric Company in Baltimore, Maryland and Patricia DANIELS is employed by the Harford County Public Schools.

23. On October 25, 2019 surveillance was conducted at 1318 Salonica Place, Bel Air (the **SUBJECT PREMISES**). At approximately 0942 hours, an adult female matching Patricia DANIELS description exited the townhouse and drove away in a Dodge van, bearing Maryland tag **7CX2823**. The van had been parked outside of the townhouse in a shared lot with numbered parking space that matched the townhouse numbers. A second spot, which also appeared to be assigned to 1318, was empty. Queries conducted through the Maryland Motor Vehicle Administration reveal that the Dodge van, bearing Maryland tag **7CX2823**, is registered to William Thomas DANIELS II at the **SUBJECT PREMISES**.

24. On February 12, 2020, I conducted surveillance at **1318 Salonica Place**, Bel Air, Maryland. At approximately 0449 hours, an individual exited the residence. A white Chevrolet Pickup truck bearing Maryland tag **14X066** was parked next to the Dodge van, bearing Maryland tag **7CX2823**. The truck had maroon writing on the door with the marking “Enterprise Electric, Baltimore” and listed the U.S. Department of Transportation number. The driver’s side front fender had the marking “290.” A query of the vehicle license plate revealed that it is registered to Williams DANIEL II’s employer, Enterprise Electric Company, at 4204 Shannon Drive in Baltimore, Maryland. At approximately 0450 hours, the Chevrolet Pickup truck bearing Maryland tag **14X066** exited the parking lot.

25. On February 13, 2020, I conducted surveillance at **1318 Salonica Place**, Bel Air, Maryland. At approximately 0453 hours, a male exited the residence and started the Chevrolet Pickup truck bearing Maryland tag **14X066**. At approximately 0505 hours, the male exited the residence once again, and drove away in the Chevrolet pickup truck. The Dodge van bearing Maryland tag **7CX2823** was parked in front of the townhouse.

SUMMARY

26. On or about September 14, 2019 and September 16, 2019, the Kik user “Rvpwk”

distributed and/or received child pornography in a Kik group chat and alleged that they were going to have sex with a minor. I believe that the user of the Kik account “Rvpwk” is located at the **SUBJECT PREMISIES**. The same IP addresses were consistently used to access the Kik account during the 8-day period of activity provided by Kik. Further, I believe that the owners and occupants of the **SUBJECT PREMISES** to be William and Patricia DANIELS who control the Dodge van, bearing Maryland tag **7CX2823** and the Chevrolet Pickup truck bearing Maryland tag **14X066**.

27. Based on my training and experience, and the activity of “Rvpwk” detailed above, I believe that the user of the Kik account “Rvpwk” displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography as discussed in paragraphs 6 and 7 above. Based on these characteristics, I respectfully submit there is probable cause that the **TARGET LOCATIONS** contain evidence of the distribution, receipt, and possession of child pornography. I also believe that the **TARGET LOCATIONS** will contain evidence of who user of the Kik account “Rvpwk” is, which has been accessed as recently as September 2019 to participate in the distribution, receipt and possession of child pornography.

REQUEST FOR PERMISSION TO EXECUTE BEFORE 6:00 A.M.

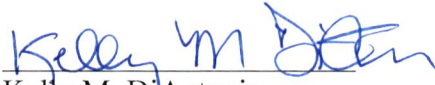
28. On February 12, 2020 and February 13, 2020, I observed an occupant of the **SUBJECT PREMISES** leave the residence and drive away in a Chevrolet Pickup truck bearing Maryland tag **14X066**, around approximately 0500 hours. A query of the vehicle license plate revealed that it is registered to the homeowner’s (Williams DANIELS II) employer, Enterprise Electric Company. Given that the child pornography was exchanged over the Kik application, which can be downloaded onto a smartphone and can be accessed virtually anywhere, it is imperative that the devices linked to the **SUBJECT PREMISES** are available during the

execution of the search warrant. As stated in paragraph 15, the child pornography distributed on September 16, 2019 was traced to a mobile IP address that resolved back to Verizon Wireless. Executing the search warrant prior to 0600 hours will reduce the potential for possible evidence to be missed.

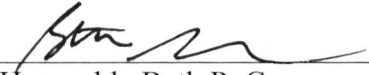
CONCLUSION

29. Based on the above information, there is probable cause to believe that 18 U.S.C. § 2252A(a)(2), which makes it a federal crime to distribute and receive child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which makes it a federal crimes to possess child pornography using a facility of interstate commerce, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses listed in Attachment B, which is incorporated herein by reference, are located in the **TARGET LOCATIONS**, as is further described in Attachments A1, A2, and A3.

30. Based upon the foregoing, I respectfully request that this Court issue search warrants for the **TARGET LOCATIONS**, more particularly described in Attachments A1, A2, and A3, authorizing the seizure of the items described in Attachment B, which are incorporated herein by reference.


Kelly M. DiAntonio
Special Agent
Homeland Security Investigations

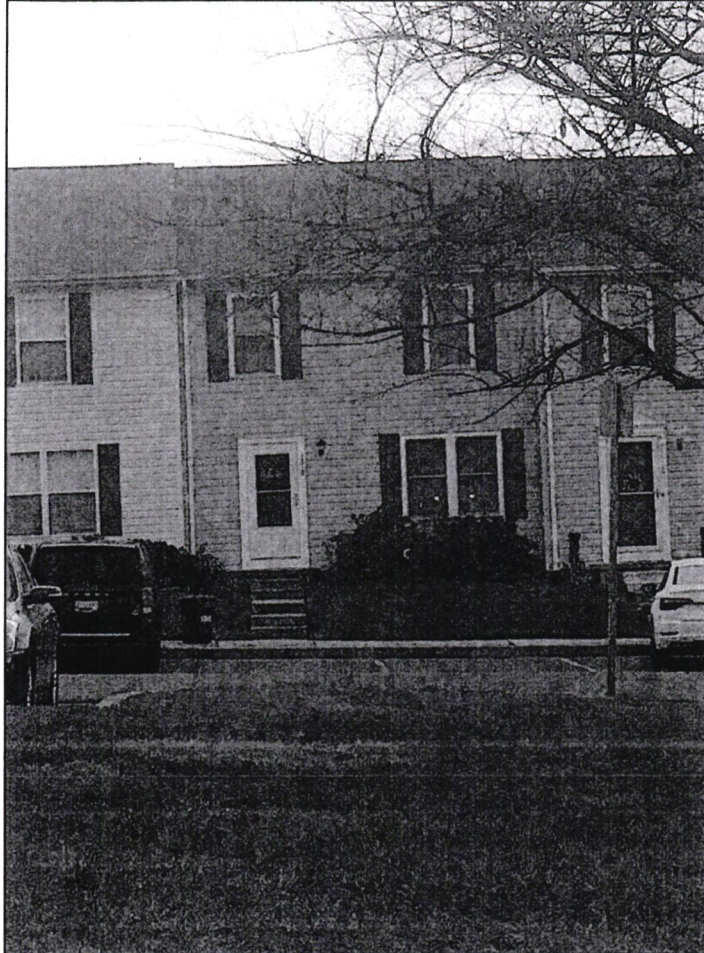
Subscribed and sworn before me this 10th day of March, 2020


Honorable Beth P. Gesner
Chief United States Magistrate Judge

20 - 0810 BPG

ATTACHMENT A1
DESCRIPTION OF PROPERTY TO BE SEARCHED

1318 Salonica Place, Bel Air, Maryland 21014 (the **SUBJECT PREMESIS**) is a two-story tan townhome with maroon shutters and a maroon front door with a white storm door. The numbers "1318" are prominently displayed in black numbering in the top corner of the door frame. A digital photograph is included below:



20 - 0811 BPG

ATTACHMENT A2
DESCRIPTION OF VEHICLE TO BE SEARCHED

This warrant applies to the vehicle further described as a dark colored **2016 Dodge Minivan** with **Maryland tag 7CX2823**.



ATTACHMENT A3
DESCRIPTION OF VEHICLE TO BE SEARCHED

This warrant applies to the vehicle further described as a **White Chevrolet Pickup Truck with Maryland tag 14X066**. The truck has maroon writing on the driver's side door with the marking "Enterprise Electric, Baltimore" a U.S. Department of Transportation number. The driver's side front fender had the marking "290."



ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED

All records, documents, items, data and other information that may constitute fruits or instrumentalities of, or contain evidence related to, violations of Title 18, United States Code, Section 2252A(a)(2), and 2252A(a)(5)(B), including, but not limited to, the following that may be found in the locations described in Attachment A1, A2, and A3:

1. Any and all cellular telephones with cameras and/or Internet capability, web cameras, cameras, film, videotapes, video recording devices, video recording players or other photographic or video equipment.
2. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to, this crime. The following definitions apply to the terms as set out in this affidavit and attachment:
 - a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data processing devices (including but not limited to central processing units, laptops, tablets, eReaders, notes, iPads, iPods, personal data assistants, cellular telephones; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
 - b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
 - c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
 - d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touches.

Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

3. Any and all images, videos, notes, documents, records, or correspondence pertaining to minors engaged in sexually explicit conduct.
4. Any and all records, documents, invoices and materials that concern any online accounts including Facebook, Instagram, Skype, or any other account that allows chatting, email, or video chats over the Internet, including screen names and email accounts.
5. Any and all records, documents, invoices and materials that concern any accounts with Internet Service Providers.
6. Any and all diaries, notebooks, notes, pictures, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.
7. Any and all documents, records, or correspondence pertaining to occupancy at 1318 Salonica Place, Bel Air, Maryland 21014.
8. Any and all notes, documents, records, or correspondence, including images or videos, that indicate a sexual interest in children or communications with children regarding sexual activity, including, but not limited to:
 - a. Correspondence with children;
 - b. Any and all visual depictions of minors;
 - c. Internet browsing history;
 - d. Books, logs, diaries and other documents.
9. Any and all records, documents, or correspondence relating to persuading, inducing, enticing or coercing any minor to engage in any sexual activity in violation of the law.
10. Any and all records, documents, or correspondence relating to transmitting obscene materials to minors.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

For any computer, computer hard drive, or other physical object upon which computer data can be recorded, which includes cellular phones, tablets, iPods, and other electronic devices

(hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.

11. *With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.*

12. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read

by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- c. “scanning” storage areas to discover and possibly recover recently deleted files;
- d. “scanning” storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

13. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.